

SPAMM Y CORREO BASURA

Te quita tiempo, satura tu buzón, infecta con virus tu equipo, intentan engañarte e invitarte a ser la víctima de un fraude electrónico.

¿Quieres saber como lidiar con este molesto mal?, Lee este documento y adopta algunos o mejor aún, todos los consejos que aquí te damos.

¿QUÉ ES EL SPAMM O CORREO BASURA?

Son todos aquellos mensajes no solicitados que llegan diariamente a tu buzón, provenientes alguien que no conoces, ofreciéndote algo que no solicitaste. Y aunque existen mensajes legítimos, con fines legítimos, la mayor parte de estos no lo son, y son utilizados con fines perjudiciales como los siguientes:

- ❑ Propagación de virus y códigos maliciosos que provocan daños a tu propio equipo, y al de otras personas o empresas.
- ❑ La obtención de más cuentas de correo electrónico para ser vendidas como bases de datos a terceros para fines ilegítimos y legítimos.
- ❑ Y el mas peligroso, Phishing o “Robo de identidad”, utilizado principalmente para realizar fraudes en línea.

Pero, ¿quién me escogió para recibir spam?, nadie nos escoge, simplemente somos los receptores de uno de los millones de correos electrónicos que se envían con el fin de incrementar las posibilidades de éxito de los puntos arriba mencionados.

¿QUIÉN LOS ENVIA Y POR QUE TIENEN MI CORREO ELECTRONICO?

Proviene de personas y de empresas que tienen tu dirección de correo electrónico que han podido obtenerla por cualquiera de los siguientes medios:

- ❑ Al suscribirte en boletines o registrarte en paginas de servicios que te solicitan dicha información, y que al ser sitios de dudosa reputación fácilmente pueden vender o compartir su base de datos con otras empresas o spammers.
- ❑ Al responder o ser participe de una cadena de mensajes que pueden parecer divertidos, informativos o inofensivos, pero que tienen como finalidad captar una gran cantidad de cuentas de correo electrónico. Y solo por curiosidad la próxima vez que recibas uno de estos mensajes, tomate el tiempo de contar la cantidad de correos electrónicos que podrían ser utilizados por cualquier persona.
- ❑ En los casos mas avanzados, rastreos automáticos por medio de Bots (robots) que navegan las paginas de internet en búsqueda de cuentas de correo electrónico principalmente de empresas.

¿QUÉ HACER CONTRA EL SPAMM Y CORREO BASURA?

Existen muchas formas de frenarlo y reducirlo, en realidad, eres receptor solo de una insignificante cantidad de ellos. Todo proveedor de servicios de internet cuenta con filtros para frenar y evitar que lleguen a tu buzón cientos o miles de correos basura y spamm.

Sin embargo, las medidas y acciones que tomes hoy, determinarán en gran medida la cantidad de spamm o correo basura que recibirás el día de mañana. Por ello compartimos contigo algunas medidas que puedes adoptar fácilmente para protegerte a ti y a los demás de este molesto mal.

1. No compartas con cualquiera tu dirección de correo electrónico principal, utiliza siempre una segunda cuenta de correo electrónico de poca importancia para asuntos de poca relevancia. Si en tu trabajo te proporcionan una cuenta de correo electrónico, recuerda que te están dando una herramienta de trabajo, y por lo tanto, debes de usarla de forma responsable.
2. Si eres parte de una empresa y debes publicar tus cuentas de correo en el sitio web de la misma. Solicita a tu proveedor o departamento de sistemas que las publiquen de forma segura. Uno de los métodos más seguros para esto, es que sean publicadas como imagen y no como texto. No olvides que una cuenta de correo es como un número telefónico, una vez creado no te conviene cambiarlo.
3. Consulta y lee siempre las políticas de privacidad de cualquier servicio en línea en el que desees participar o registrarte, de otra forma podrías estar autorizando que de forma indiscriminada tu información sea compartida con terceros.
4. Protege a tus destinatarios; para ello todo software de correo electrónico cuenta con casillas etiquetadas como **BCC** o **CCO** (Copia carbón oculta), de esta forma todo mensaje que envíes protegerá la identidad de los destinatarios de la vista de los demás.
5. No abras archivos adjuntos si no conoces su contenido o veracidad, no importa que provengan aparentemente de un conocido, es muy fácil cambiar la identidad de un correo electrónico. Recuerda que unos segundos de risa, un minuto de reflexión o una información vaga, podría hacerte pasar un mal rato a ti o a las personas en tu lista de contactos.
6. No reenvíes mensajes en cadena a toda tu lista de contactos. Además de que estarás haciendo pública tu cuenta de correo a una infinidad de personas, podrías estar participando en la distribución de un virus o un código malicioso. Debes elegir siempre a cada uno de tus destinatarios y respetar a quien no desee recibirlos.
7. Evita ser receptor de cadenas. Recuerda que otra persona podría no tomarse la molestia de proteger tu identidad y tu cuenta de correo electrónico.
8. Desconfía de aquellos correos que provengan de bancos, sitios web o instituciones que te inviten a proporcionar nombres de usuario y contraseñas. Si eres usuario de estos servicios, nunca accedas a ellos dando clic en el correo electrónico, siempre teclea manualmente la dirección en tu navegador.

9. Si recibes correos electrónicos de personas que no conoces, con asuntos o en idiomas que no tienen relación contigo. Simplemente ignóralos y elimínalos sin abrirlos. El simple hecho de abrirlos puede dar señal de que has recibido el mensaje, y estarás confirmando que puedes recibir más.
10. Evita caer en estafas, hoy día existen miles de casos que solicitan tu apoyo, comprensión o ayuda solicitándote que reenvíes un correo a todos tus contactos. Si en realidad deseas ayudar, comunícate directamente con la persona o institución para informarte como puedes apoyarles. De otra manera, podrías estar contribuyendo a que todos tus contactos reciban más spam y correo basura, y que puedan ser víctimas de un daño a su equipo, o peor aun, de un fraude electrónico.

¿QUÉ MAS PUEDO HACER?

Queda claro que podemos ser afectados por terceros de forma involuntaria, por ello es que debemos contar con un antivirus y tratar de tener un firewall o cortafuegos para impedir que código malicioso pueda hacer de las suyas. Y para esto te recomendamos el siguiente software, aunque existen otras alternativas en el mercado.

AVG Anti-Virus : <http://www.grisoft.com>

Zone Alarm : <http://www.zonealarm.com/>

Según sea tu caso, recuerda siempre lo siguiente ..

- ❑ Como dueño de un equipo de computo, esto permitirá que tengas un equipo mas limpio, eficiente y podrás evitar costosas reparaciones.
- ❑ Como empleado de una empresa, estos consejos te podrán evitar desde llamadas de atención, penalizaciones o hasta la perdida de tu propio empleo.
- ❑ Y como dueño o responsable de una empresa o administrador del equipo de computo de la misma, adoptar estos y otros consejos como normas del buen uso del correo electrónico pueden evitarte grandes dolores de cabeza y darle grandes ahorros económicos a la empresa.

Si quieres conocer más sobre este tema puedes dirigirte a las siguientes direcciones de internet de donde se han extraído conceptos e ideas para este documento.

Departamento de Seguridad en Cómputo: <http://www.seguridad.unam.mx>

Navega Protegido en Internet : <http://www.navegaprotegido.org.mx>

Este documento esta a tu disposición en nuestro sitio web en la siguiente dirección:
<http://www.izaris.com/soporte>

Soporte Técnico IZARIS
soporte@izaris.com